BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PESSOAIS

2024

MINISTÉRIO DO PLANEJAMENTO ORÇAMENTO

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

MINISTÉRIO DO PLANEJAMENTO E ORÇAMENTO – MPO

Ministra do Planejamento e Orçamento
Simone Nassar Tebet

Secretário-Executivo
Gustavo José de Guimarães e Souza

Encarregada pelo Tratamento de Dados Pessoais
Carolina Palhares Lima

Elaboração
Carolina Palhares Lima
Ianê de Andrade Azevedo
Amanda Machado Gazolla
Yarin Santos de Melo

Projeto gráfico e arte (Ouvidoria/MPO)
Jéssica Ellen Azevedo Orion Lopes
Carolina Palhares Lima

Informações
E-mail: lgpd.mpo@planejamento.gov.br

Ministério do Planejamento e Orçamento
gov.br/planejamento
@MinPlanejamento
@planejamentoeorcamento

2024

SUMÁRIO

Esse guia de Boas Práticas tem por objetivo orientar os profissionais do Ministério do Planejamento e Orçamento (MPO) na aplicação da Lei Geral de Proteção de Dados (LGPD - Lei n° 13.709/2018), disponibilizando noções gerais sobre a Lei e fornecendo orientações e boas práticas sobre as operações de tratamento de dados pessoais.

A LGPD dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade dos indivíduos. A Lei se aplica a qualquer tratamento de dados pessoais, independentemente do meio (físico ou digital) ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional.

Assim, a LGPD trata, fundamentalmente, de medidas para **gestão dos riscos do processo de tratamento de dados pessoais**, de forma que a administração pública possa controlar e mitigar esses riscos ao garantir o atendimento dos princípios e a utilização das hipóteses de tratamento previstas na Lei, bem como ao instituir uma cultura de proteção de dados e de privacidade desde a concepção e ao definir: 1) a governança da proteção de dados; 2) os controles necessários para o compartilhamento de dados; 3) os mecanismos de transparência e garantia dos direitos do titular e; 4) a obrigatoriedade de comunicação de incidentes.

Nesse contexto, é fundamental que todo tratamento de dados pessoais somente seja realizado se atender a uma das hipóteses de tratamento (arts. 7º e 11 da LGPD) e se houver uma finalidade específica para a operação de dados pessoais, limitando-se a coleta, o acesso e o tempo de tratamento dos dados ao mínimo necessário. Além disso, devem ser tomadas medidas preventivas e de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

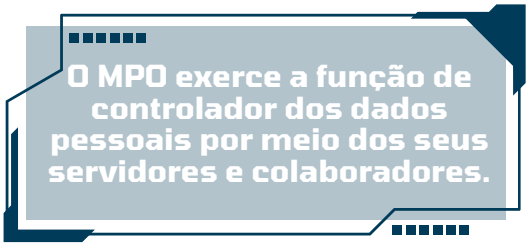
A realização de ações de comunicação e capacitação é outra boa prática essencial para difundir informações sobre a implementação da LGPD e para fomentar a cultura de proteção de dados na instituição.

CONCEITOS

Para melhor compreensão da Lei Geral de Proteção de Dados e das orientações contidas nesse documento, estão relacionados a seguir os principais conceitos relativos ao tema.

- **Agentes de tratamento:** o controlador e o operador (inciso IX do art. 5º da LGPD).

- **Autoridade Nacional de Proteção de Dados (ANPD):** instituição responsável por, dentre outros pontos, zelar, elaborar diretrizes e editar regulamentos e procedimentos para a proteção de dados pessoais, bem como por fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.



- **Coleta de dados pessoais:** etapa inicial do tratamento de dados realizada para obtenção dos dados pessoais do cidadão (titular dos dados), a qual somente deve ser realizada mediante o atendimento das hipóteses de tratamento, das medidas de segurança, dos princípios, dos diretos do titular e das demais regras dispostas pela LGPD.

- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (inciso VI do art. 5º), tais como definir a forma como o tratamento será realizado, as medidas para garantir a transparência e manter o registro das operações de tratamento, assim como designar o encarregado pelo tratamento de dados pessoais. O MPO exerce a função de controlador dos dados pessoais por meio dos seus servidores e colaboradores.

- **Dados pessoais:** são os dados relacionados a pessoa natural identificada ou identificável, ou seja, que identificam ou podem identificar um indivíduo, podendo incluir o nome, RG, CPF, endereço, e-mail, número de telefone, dentre outros.

- **Dados pessoais sensíveis:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (inciso II do art. 5º).

- **Direitos do titular:** o titular dos dados tem direito de obter informações sobre como os seus dados pessoais são tratados e de realizar solicitações ou reclamações junto ao controlador. Informações adicionais sobre o tema estão disponíveis em tópico específico desse documento.

- **Encarregado:** pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD (inciso VIII do art. 5º). Compete ao encarregado: 1) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; 2) receber comunicações da autoridade nacional; e 3) orientar os profissionais do órgão a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. No MPO, atualmente a Ouvidora exerce o encargo de encarregada pelo tratamento de dados pessoais.

- **Hipótese de tratamento de dados pessoais:** as hipóteses de tratamento de dados pessoais previstas na Lei Geral de Proteção de Dados estabelecem as situações que autorizam o uso de dados pessoais (arts. 7º e 11). Informações adicionais sobre o tema estão disponíveis em tópico específico desse guia de Boas Práticas.

- **LGPD**: Lei Geral de Proteção de Dados Pessoais.

- **Operador: o**perador é o agente responsável por realizar o tratamento de dados pessoais em nome do controlador e conforme a finalidade por este delimitada. Assim, o operador é pessoa natural ou jurídica, de direito público ou privado, ao qual compete realizar e registrar o tratamento de dados pessoais segundo as instruções fornecidas pelo controlador, devendo, também, seguir o que estabelece a LGPD. Sempre que houver compartilhamento de dados pessoais com terceiros (ex.: empresa contratada para consultoria ou execução de serviços), esse terceiro é considerado operador, pois atua em nome do controlador (o MPO), seguindo suas orientações.

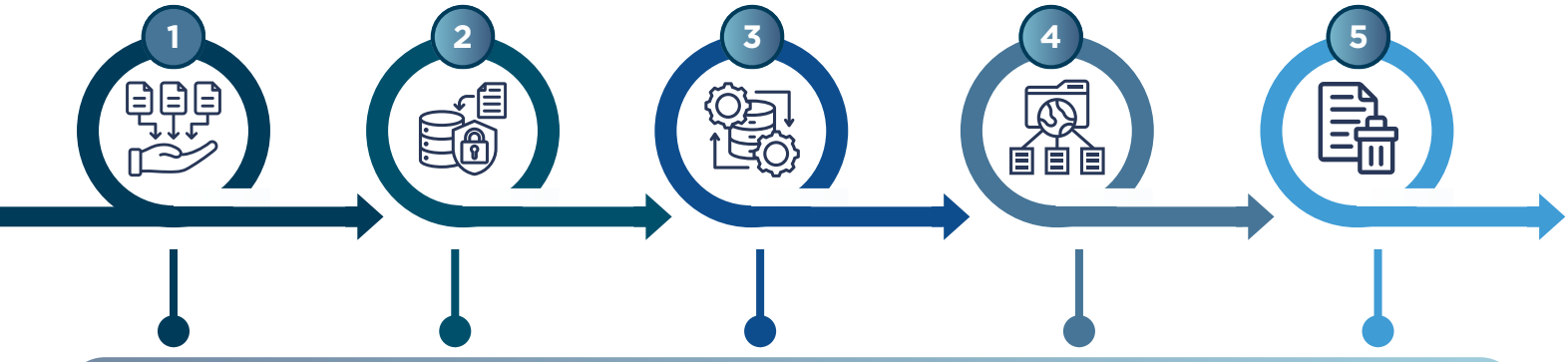
- **Relatório de Impacto à Proteção de Dados Pessoais (RIPD):** documento que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como contém as medidas, salvaguardas e mecanismos de mitigação de riscos (inciso XII do art. 5º).

- **Tempo de tratamento de dados pessoais:** duração do ciclo de vida dos dados pessoais, desde a coleta até a eliminação ou arquivamento/armazenamento.

- **Titular dos dados pessoais:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (inciso V do art. 5º).

- **Tratamento de dados pessoais:** toda operação realizada com dados pessoais, como as que se referem à coleta, retenção, processamento, compartilhamento e eliminação dos dados (ciclo de vida dos dados pessoais). Consiste na utilização dos dados pessoais dos titulares para uma finalidade específica. O conjunto das fases de tratamento é denominado ciclo de vida dos dados pessoais.

CICLO DE VIDA DOS DADOS PESSOAIS



COLETA	RETENÇÃO	PROCESSAMENTO	COMPARTILHAMENTO	ELIMINAÇÃO
Coleta, recepção ou produção de dados pessoais	Arquivamento ou armazenamento de dados pessoais.	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.	Transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais	Apagamento ou eliminação de dados pessoais

PRINCÍPIOS DA LGPD

A LGPD elenca princípios que devem obrigatoriamente ser observados no tratamento de dados pessoais (art. 6º). Desse modo, uma vez identificada a hipótese de tratamento aplicável, é fundamental garantir que os princípios da LGPD sejam respeitados, sendo necessário:

1)Identificar a **finalidade** para a qual o tratamento de dados é realizado.

2)Limitar o tratamento dos dados ao **mínimo necessário**, minimizando a coleta, o acesso e o tempo de tratamento.

3)Definir e documentar as medidas **preventivas** e de **segurança**, técnicas e administrativas, adotadas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, bem como para proteger os dados de acessos não autorizados, de situações acidentais ou ilícitas e de uso para fins **discriminatórios.**

4)Demonstrar que o órgão está aderente à LGPD, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto a sua eficácia (**responsabilização e prestação de contas**).

Ainda com o intuito de atender aos princípios da LGPD e de garantir os direitos do titular dos dados, deve-se:

1)Informar ao titular sobre o tratamento realizado e a **finalidade** à qual ele se destina.

2)Garantir que o tratamento dos dados está **adequado** à finalidade informada.

3)Garantir a **transparência** das informações de maneira que os titulares possam ter **livre acesso**, por meio de consulta ou requisição (transparência ativa ou passiva), a informações claras e precisas sobre o tratamento de seus dados pessoais (conteúdo, forma, duração, compartilhamento, agentes de tratamento etc.).

4)Garantir a **qualidade dos dados** tratados (exatidão, clareza, relevância e atualização dos dados).

HIPÓTESES DE TRATAMENTO

A LGPD permite que a administração pública realize o tratamento de dados pessoais unicamente para o atendimento de finalidade pública, observando sempre o interesse público, e prevê as **situações que autorizam o tratamento de dados pessoais,** as quais são denominadas hipóteses de tratamento (arts. 7º e 11).

Nesse contexto, **o tratamento de dados pessoais pela administração pública e pelo MPO independe de consentimento do titular,** pois é, fundamentalmente, realizado nas hipóteses de: 1) cumprimento de obrigação legal ou regulatória; ou 2) execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (incisos II e III do art. 7º e alíneas "a" e "b" do inciso II do art. 11 da LGPD).

Ainda que não exista a necessidade de consentimento, todos os direitos dos titulares devem ser garantidos (ver tópico a seguir).

SAIBA MAIS: Para mais informações sobre as hipóteses de tratamento de dados pessoais e dados pessoais sensíveis, acesse os artigos 7º e 11 da LGPD.

DIREITOS DO TITULAR DOS DADOS

Todo cidadão (titular dos dados) tem o direito de obter informações sobre como os seus dados pessoais são tratados e utilizados no MPO. Para o exercício dos direitos dos titulares, a Lei prevê um conjunto de mecanismos que se traduzem, fundamentalmente, em obrigações de transparência ativa e passiva e na definição de meios processuais para provocar a administração pública.

Alguns desses direitos são exercidos por meio do acesso a informações disponibilizadas na página eletrônica do MPO (transparência ativa), tais como finalidade, forma e duração do tratamento, assim como identificação e informações de contato do controlador (art. 9º).

Outros direitos são exercidos por meio de pedido de acesso à informação (transparência passiva) e, portanto, submetem-se aos prazos e procedimentos já estabelecidos pela Lei de Acesso à Informação (LAI - Lei nº 12.527/2011), podendo ser solicitadas, entre outras, informações quanto à confirmação da existência de tratamento; ao acesso aos dados de que é titular e que são objeto de tratamento; e às entidades públicas e privadas com as quais foi realizado uso compartilhado de dados (arts. 18 a 20 da LGPD).

A LAI, no entanto, não é uma referência exclusiva para o exercício dos direitos dos titulares, que também podem se manifestar por meio do envio de solicitações de providências e de reclamações à Ouvidoria/MPO, pela **plataforma Fala.BR**, requisitando, entre outras questões, a correção de dados incompletos, inexatos ou desatualizados e a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18).

O titular de dados pode entrar em contato com o MPO e a encarregada pelo tratamento de dados pessoais pelo **Fala.BR**, enviando um pedido de acesso à informação (LAI) ou uma manifestação de ouvidoria (solicitação de providências ou reclamação).

Outras formas de o titular dos dados entrar em contato com o MPO estão disponíveis na página eletrônica do Ministério.

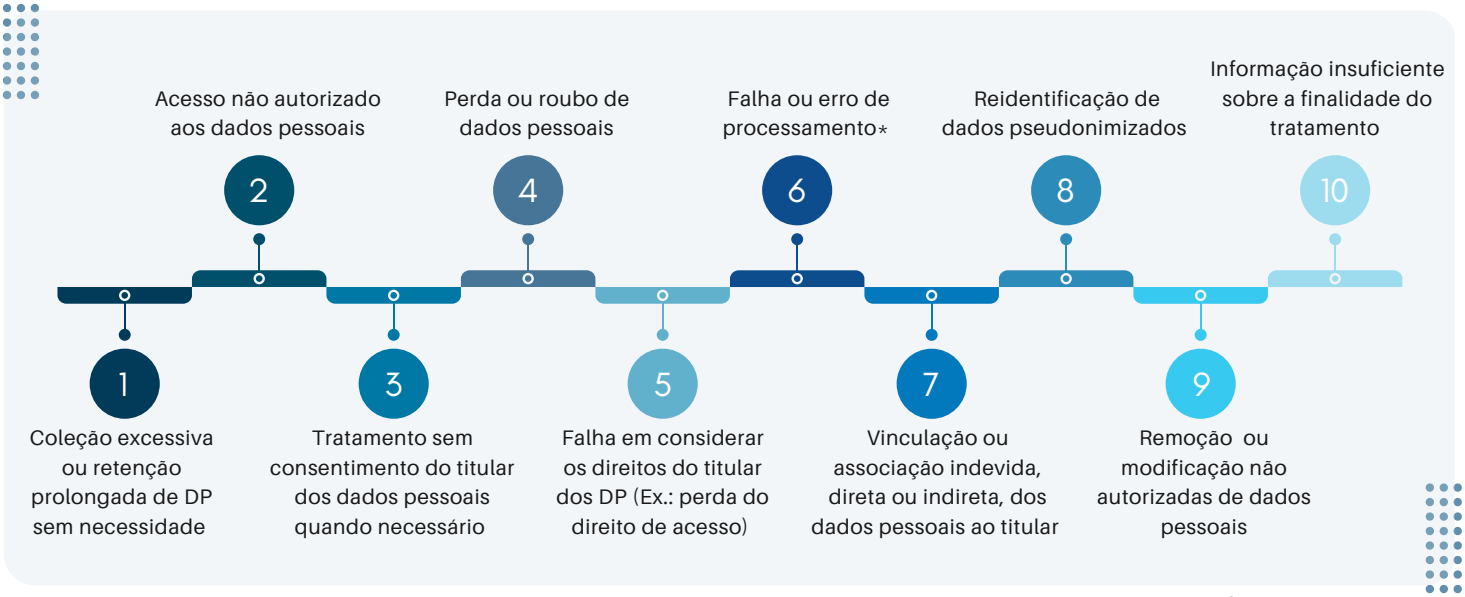
GESTÃO DE RISCOS DO TRATAMENTO DE DADOS PESSOAIS

Riscos relacionados ao tratamento de dados pessoais

Risco pode ser definido como a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos da organização. O gerenciamento de riscos consiste, assim, na identificação, avaliação e controle de potenciais eventos ou situações, de forma a aumentar a probabilidade de alcance dos objetivos de um processo.

Nesse sentido, o gerenciamento dos riscos do processo de tratamento de dados pessoais permite que sejam identificados os riscos e as medidas necessárias para controle desses riscos, com o intuito de garantir a proteção dos dados pessoais.

A seguir estão listados possíveis riscos de privacidade e de segurança da informação relacionados ao tratamento de dados pessoais:



* Falha ou erro de processamento - ex: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada.

SAIBA MAIS: Para mais informações sobre os riscos ligados ao tratamento de dados pessoais, acesse o Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD).

Relatório de Impacto à Proteção de Dados Pessoais - RIPD

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é um documento previsto na LGPD que contém a descrição dos processos de tratamento de dados pessoais, os riscos associados ao tratamento e as medidas para controle desses riscos. O RIPD representa um importante instrumento de análise e documentação da conformidade do tratamento de dados pessoais realizado pela instituição.

Esse relatório deve, idealmente, ser elaborado antes do início do tratamento de dados pessoais e, no MPO, sua elaboração deve estar compatível com a Política (Resolução SRTCI/MPO nº 1, de 28 de setembro de 2023) e a Metodologia de Gestão de Riscos do Ministério.

O RIPD não é necessário para todo processo de tratamento de dados pessoais. Sua elaboração ou atualização está indicada, entre outras situações, sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais resultante de:

- tratamento de dados pessoais sensíveis (LGPD, art. 5º, II);
- tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);
- tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42).

De acordo com a LGPD (art. 38), o RIPD deve conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

SAIBA MAIS: Para mais informações sobre o RIPD e suas etapas de elaboração, acesse o Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD) - Comitê Central de Governança de Dados, 2020.

Medidas de controle dos riscos

A definição e a implementação de medidas de controle dos riscos do processo de tratamento são essenciais para a garantia da proteção de dados pessoais. A seguir, estão listadas algumas dessas medidas:

Minimização

O tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades. Dessa forma, devem ser coletados e tratados somente os dados necessários ao cumprimento da finalidade a que se propõe.

Princípio do privilégio mínimo

O princípio do privilégio mínimo determina que os usuários de um sistema de informação ou base de dados devem receber acesso apenas aos dados e às operações de que efetivamente necessitam para executar seus trabalhos. Desta forma, o acesso a dados pessoais deve ser restrito ao mínimo necessário para a realização da operação de tratamento.

"Restrição de acesso" aos dados pessoais

No âmbito da Lei de Acesso à Informação (LAI), define-se que as informações pessoais relativas à intimidade, vida privada, honra e imagem terão seu acesso restrito a agentes públicos legalmente autorizados e à pessoa a que elas se referirem. Além disso, esses dados poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

SAIBA MAIS: Para mais informações sobre o RIPD e suas etapas de elaboração, acesse o Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD) - Comitê Central de Governança de Dados, 2020.

Pseudonimização e anonimização

Um dado anonimizado é aquele relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (inciso III do art. 5º da LGPD). Os processos de anonimização e pseudominização podem ser utilizados com o intuito de proteger os dados pessoais, reduzindo os riscos de identificação dos indivíduos, quando necessário.

- **Pseudonimização:** Tratamento por meio do qual os dados somente podem ser associados a um titular mediante a utilização de informações adicionais mantidas separadamente pelo controlador em ambiente controlado e seguro. Essa técnica deve ser utilizada quando se quer evitar a identificação de um titular através de seus dados pessoais, mas ainda se pretende manter possível a sua reidentificação.

- **Anonimização:** Procedimento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. A partir do momento em que o dado é considerado anonimizado e não permite mais qualquer identificação do seu titular, este dado sai do escopo da LGPD, por não mais se tratar de um dado pessoal. Essa técnica deverá ser utilizada quando não se pretende mais reidentificar o titular dos dados pessoais.

Cuidados no compartilhamento de dados pessoais

O compartilhamento de dados pessoais consiste na transferência de informações entre organizações públicas ou entre uma organização pública e um terceiro privado. **O uso compartilhado** de dados pessoais pelo MPO deve atender à finalidade para a qual os dados foram coletados e, quando realizado com terceiros, **deve ser documentado e formalizado em contrato ou instrumento similar.**

Nos casos de compartilhamento com terceiros privados, o órgão contratante (controlador) não apenas estabelecerá a finalidade do tratamento, mas também exigirá da empresa contratada (operador) a adoção dos meios técnicos necessários para **garantir a observância dos princípios que regem o tratamento dos dados pessoais (art. 6º da LGPD).** Além disso, o compartilhamento deve se ater ao estritamente necessário para atender à finalidade estabelecida, atentando-se para a **minimização de dados** quanto aos dados compartilhados (compartilhar o mínimo necessário), ao acesso (dar acesso ao menor número possível de pessoas) e ao tempo de retenção (tratar os dados pelo mínimo de tempo possível).

Ao término do tratamento dos dados compartilhados, é importante **que eles sejam eliminados. Caso ocorra um incidente de segurança** com os dados, o operador também tem a responsabilidade de **reportá-lo** ao controlador e ao encarregado de dados.

Quando o compartilhamento é realizado com país estrangeiro ou organismo internacional, ocorre a transferência internacional de dados, para a qual há requisitos adicionais (arts. 33 a 36 da LGPD), pois somente é permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD e, entre outros condicionantes, quando o controlador garantir o cumprimento dos direitos do titular e do regime de proteção de dados e dos princípios previstos na lei.

Tempo de retenção

A retenção corresponde ao arquivamento ou armazenamento de dados pessoais e ela deve ocorrer por tempo limitado. Dessa forma, ao se finalizar o tratamento dos dados, estes deverão ser eliminados. Nos termos da LGPD (art. 15), o término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Para apoiar a definição do tempo de retenção de um dado pessoal e organizar os documentos de maneira eficiente, pode ser utilizada a tabela de temporalidade e destinação que define por quanto tempo cada documento deve ser guardado e qual será seu destino final: descarte ou arquivamento permanente. Essa tabela deve incluir todos os documentos criados ou recebidos por um órgão ou entidade pública no exercício de suas atividades.

SAIBA MAIS: Para mais informações sobre o tempo de retenção de dados pessoais você também pode conferir a tabela de temporalidade do Conselho Nacional de Arquivos (CONARQ).

Resposta aos incidentes

O monitoramento, a notificação e a resposta a incidentes com dados pessoais são importantes mecanismos para a identificação e o controle dos impactos de um evento. Informações adicionais sobre esse tema estão disponíveis no Tópico COMUNICAÇÃO DE INCIDENTES.

Considerando a necessidade de mitigar incidentes com dados pessoais, devem ser adotadas medidas de segurança, técnicas e administrativas, aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (art. 46 da LGPD).

As seguintes medidas técnicas e organizacionais de privacidade e proteção de dados foram propostas no Modelo de Política de Proteção de Dados Pessoais:

- O acesso aos dados pessoais deve estar limitado as pessoas que realizam o tratamento.
- As funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais devem ser claramente estabelecidas e comunicadas.
- Devem ser estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais.
- Todos os dados pessoais devem estar armazenados em ambiente seguro, de modo que terceiros não autorizados não possam acessá-los.

COMUNICAÇÃO DE INCIDENTES

Incidente de segurança é qualquer evento relacionado à violação na segurança de dados pessoais. Caso um incidente de segurança venha a ocorrer, a encarregada de dados pessoais deverá ser comunicada pelos profissionais que tratam os dados (controlador e operador), para que, na sequência, ela comunique o incidente à ANPD.

Ao identificar um incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o MPO deverá comunicá-lo à autoridade nacional e ao titular. Considera-se risco ou dano relevante aos titulares o evento de segurança que pode afetar significativamente interesses e direitos fundamentais dos titulares e, envolver, entre outros:

- dados pessoais sensíveis;
- dados de crianças, de adolescentes ou de idosos;
- dados em larga escala.

QUEM COMUNICA

A LGPD impõe a todos os profissionais do MPO o dever de comunicar a ocorrência de incidentes que possam causar riscos ou danos relevantes aos titulares de dados pessoais.

O QUE COMUNICAR

Um incidente precisa ser comunicado se atender aos seguintes critérios:

- **Tenha a ocorrência confirmada pelos agentes de tratamento;**
- **Envolva dados pessoais sujeitos à LGPD; e**
- **Acarrete risco ou dano relevante aos titulares dos dados.**

COMO COMUNICAR

A comunicação imediata de um incidente deve ser realizada à encarregada pelo tratamento de dados pessoais do MPO pelos seguintes canais:

Telefone: (61) 2020-5113

E-mail: lgpd.mpo@planejamento.gov.br

SAIBA MAIS: Para mais informações sobre a comunicação de incidentes de segurança confira o art. 48 da LGPD, a resolução CD/ANPD nº 15, de 24 de abril de 2024 e o Guia de Resposta a Incidentes.

CONCLUSÃO

A proteção dos dados pessoais deve ser garantida durante todo o ciclo de vida do processo de tratamento dos dados, desde a sua coleta até a sua eliminação (privacidade desde a concepção), o que é possível a partir de uma abordagem constante que envolva a gestão e o manejo dos riscos do processo.

A LGPD estabelece requisitos e regras para o tratamento de dados pessoais realizado pela administração pública, buscando garantir a proteção dos dados por meio da implementação de controles dos riscos associados a esse tratamento. Desse modo, medidas preventivas e de segurança, técnicas e administrativas, devem ser adotadas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, bem como para proteger os dados de acessos não autorizados, de situações acidentais ou ilícitas e de uso para fins discriminatórios.

Assim, a realização de tratamento de dados pessoais no MPO deve atender a uma finalidade específica e limitar-se ao mínimo necessário de dados coletados, de tempo de tratamento e de acesso aos dados. O tratamento de dados pessoais deve ser registrado (art. 37 da LGPD) por meio da realização do mapeamento do processo e da elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), quando for o caso.

Quando houver compartilhamento de dados, é importante garantir que o operador adote medidas de proteção de dados e atenda aos princípios da LGPD. No caso de terceiros privados, é fundamental que o compartilhamento seja formalizado e que estejam claramente definidos os papéis do controlador (contratante) e do operador (contratado), atentando-se sempre à minimização dos dados compartilhados, à sua eliminação ao final do tratamento e à obrigatoriedade de reporte, ao MPO, de eventuais incidentes com os dados pessoais.

Para garantia dos direitos dos titulares, deve ser dada transparência e ser definido mecanismo de consulta que lhes permita livre acesso às informações quanto ao tratamento de seus dados pessoais.

No caso de ocorrência de incidente com dados pessoais, além das medidas para controle do incidente e redução de seus impactos, a encarregada pelo tratamento de dados pessoais deve ser informada e, na sequência, a ANPD e os titulares dos dados também serão comunicados.

Em síntese, as boas práticas trazidas nesse documento fazem parte da estratégia de comunicação e capacitação do corpo técnico do Ministério e visam contribuir para a criação da cultura de privacidade no órgão.

REFERÊNCIAS BIBLIOGRÁFICAS

- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
- Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI) - Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal e dá outras providências.
- Portaria de Pessoal GM/MPO nº 585/2023 - Designa a Ouvidora Carolina Palhares Lima para exercício do encargo de Encarregada pelo Tratamento de Dados Pessoais no âmbito deste Ministério, nos termos da Lei nº 13.709, de 14 de agosto de 2018.
- Resolução CD/ANPD nº 18, de 16 de julho de 2024 - Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.
- Resolução CD/ANPD nº 15, de 24 de abril de 2024 - Aprova o Regulamento de Comunicação de Incidente de Segurança.
- Decreto nº 7.724/2022 - Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.
- Decreto nº 10.406/2019 - Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.
- Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD) - Comitê Central de Governança de Dados, 2020.
- Guia Orientativo dos Agentes de Tratamento de Dados Pessoais e do Encarregado pela ANPD.
- Ato TRT5 N. 486/2022 - Institui a Política de Privacidade e Proteção de Dados Pessoais do Tribunal Regional do Trabalho da 5ª Região.
- Código de classificação e tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal.
- Modelo de Política de Proteção de Dados Pessoais – Programa de Privacidade e Segurança da Informação (PPSI).
- Guia Metodológico para Gestão de Riscos- Ministério do Planejamento e Orçamento – MPO, 2024.